December 2004

Alleviating Consumers' Privacy Concerns in Location-Based Services: A Psychological Control Perspective

Heng Xu
National University of Singapore

Hock-Hai Teo
National University of Singapore

ALLEVIATING CONSUMERS' PRIVACY CONCERNS IN LOCATION-BASED SERVICES: A PSYCHOLOGICAL CONTROL PERSPECTIVE

Heng Xu and Hock-Hai Teo
Department of Information Systems
National University of Singapore
Singapore
xuheng@comp.nus.edu.sg **teohh@comp.nus.edu.sg**

Abstract

Location-based services (LBS), enabled by advances in mobile and positioning technologies, have afforded users with a pervasive flexibility to be uniquely addressable and to access network and services on-the-move. However, because LBS could also associate the lifestyle habits, behaviors, and movements with a consumer's personal identity, privacy concerns are particularly salient for LBS. Drawing on psychological control and privacy literature, we designed an experiment study to test the basic proposition that the assurance of consumers' perceived control over their personal information has a considerable influence on alleviating their privacy concerns. Three different mechanisms of assurance of control—technology, industry self-regulation, and legislation—were manipulated in the experiment, and their effects on consumers' privacy concerns were examined. The results indicated that the technological assurance mechanism (i.e., mobile device in this study) played the most important role in assuring consumers' perceived control over personal information. The marriage of the privacy and psychological control literature streams provides a rich understanding of consumers' privacy reaction to LBS usage and, therefore, benefits the privacy and human-computer interaction (HCI) research in the Information Systems discipline.

Keywords: Location-based services, LBS, information privacy, psychological control, human-computer interaction, HCI

Introduction

The recent proliferation of mobile communication technologies has fueled a booming transformation of electronic commerce applications for the mobile arena. The development of positioning technologies, such as the global positioning system (GPS) and sophisticated cellular triangulation techniques, has not only provided consumers with unprecedented accessibility to network services while "on the move," but also enabled the localization of services (Sharma and Deng 2002). Those commercial location-sensitive applications and services that utilize geographic positioning information to provide value-added services are termed location-based services (LBS), and are marketed under the term L-Commerce (Gidari 2000).

The commercial potential and rapid growth of LBS have been accompanied, however, by concerns regarding the collection and dissemination of consumer information by service providers and merchants. These concerns pertain to the confidentiality of accumulated consumer data (Gidari 2000) and the potential risks that consumers will experience over the possible breach of confidentiality (Beinat 2001). Moreover, "location information reveals the position of a person often in real time, and thus the intrusion potential and privacy concern are more critical than with other types of personal information" (Beinat 2001, pp. 14-15). The convenience of LBS notwithstanding, consumers worry about such privacy intrusions; Bienat (2001) found that 24 percent of potential LBS users are seriously concerned about the privacy implications of disclosing their location. Privacy concern thus becomes a major inhibiting factor in consumers' adoption of LBS (Beinat 2001; Gidari 2000). Therefore, it is crucial for us to

make a response to the call of "no L-Commerce without L-privacy" (Gidari 2000) by identifying the appropriate assurance mechanisms that could assuage privacy concerns in the LBS context.

A significant body of research in privacy and information systems has suggested that concern about information privacy is one of the most important issues in today's technology-based environment (Stone and Stone 1990). Extant literature in privacy studies posits that psychological control is a precondition for protecting privacy. For example, Wolfe and Laufer (1974) have suggested that the need and ability to exert control over self, objects, spaces, information, and behavior is a critical element in any concept of privacy. Hence, the loss of control over information is central to the notion of invasion of privacy (Stone and Stone 1990). Numerous studies on employee monitoring have also acknowledged the importance of personal control in privacy issues in the organization context (e.g., Zweig and Webster 2002).

Although prior empirical work in employee privacy research has provided a reasonable foundation for understanding the fundamentals of privacy as a personal control concept (e.g., Zweig and Webster 2002, 2003), this body of work has mainly examined how *control*, as one of the inherent *technical* characteristics of the system, can affect the perceptions of privacy invasion. Moreover, these studies have been conducted in a organization context and have focused on examining the effects of *personal control*, in which the *self* acts as the control agent, on perception of privacy invasion, while neglecting other types of perceived control which may also have impacts on privacy concerns (e.g., proxy control in which powerful others act as the control agent). To our knowledge, few studies in the consumer information privacy context have examined privacy issues by incorporating the psychological control perspectives with privacy literature. We seek to address this gap in the literature by identifying the assurance mechanisms that are useful in alleviating the privacy concerns of potential LBS adopters. In particular, we aim to contribute to the ongoing debate in consumer privacy research on the relative effectiveness of technology, industry self-regulation, and government legislation in ensuring the consumer's privacy in the LBS context (Culnan and Bies 2003). An experiment study was employed to test the basic proposition that the assurance of consumers' perceived control over their personal information has a considerable influence on alleviating their privacy concerns.

The study reported here is novel to the extent that existing empirical research in consumer privacy research has not examined privacy issues from a psychological control perspective in the LBS context. The synthesis of the privacy and psychological control literature streams may provide a rich understanding of consumers' privacy reactions to LBS usage and, therefore, benefit consumer privacy and HCI research in the Information Systems discipline. The findings are also potentially useful to privacy advocates, regulatory bodies, merchants, wireless service providers, and device manufacturers to help shape or justify their decisions concerning LBS.

Conceptual Foundation

Perceived Control

Control is being increasingly recognized as an issue that strikes at the heart of individual psychology. The construct of control has often been treated as a perceptual construct because it is of greater interest than actual control when predicting behavior (Skinner 1996). The conceptualization of perceived control, therefore, differs from the typical usage of the term *control* in the management literature in that perceived control is a cognitive construct and, as such, may be subjective (Langer 1975). Specifically, perceived control has been defined as a psychological construct reflecting an individual's beliefs, at a given point in time, in one's ability to effect a change, in a desired direction, on the environment (Greenberger and Strasser 1986). It has also been generally defined as "the extent to which an agent can produce desired outcomes" (Skinner et al. 1988).

Control Agent

Most researchers in mainstream psychology may mean personal control when they refer simply to control. For example, Skinner (1996) concluded after a comprehensive review of the control-related constructs that the prototypical control is personal control, in which the agent of control is the self. However, Yamaguchi (2001) goes beyond the simple notions of control by outlining not only personal control, but also two other types of control: proxy, and collective control. Yamaguchi explicates three types of control agents: (1) *personal control*, in which the self acts as the control agent, (2) *proxy control*, in which powerful others act as the control agent, and (3) *collective control*, in which the collective acts as the control agent.

People who value autonomy would prefer exercising direct *personal control* as they "would especially feel themselves more self-efficacious when their agency is made explicit" (Yamaguchi 2001, p. 226). However, when exercise of personal control is neither readily available nor encouraged, people might well relinquish their direct control preferences and seek "security in proxy control" (Bandura 1982, p. 142). *Proxy control* is an attempt to align oneself with a powerful force in order to gain control through powerful others when people do not have enough skills, resources, and power to bring about their desired outcome or to avoid an undesired outcome in the environment (Yamaguchi 2001). For example, in the situation of third-party interventions in which intermediaries are called upon to regulate the relationships between parties with potential or actual conflict of interests, people can gain a desired outcome with the help of those intermediaries without acting like an agent (i.e., proxy control). The third type of control is *collective control* in which the individual attempts to control the environment as a member of a group or collective (Yamaguchi 2001). In collective control, responsibility and agency will be diffused among all actors (Latane and Darley 1970) and thus everyone in a collective is responsible for the outcome to the same extent.

Privacy as Psychological Control

Prior research has repeatedly shown information privacy to be of utmost concern in diverse organizational and marketing contexts and it is argued that information privacy continues to be eroded as a result of technology innovations (Stone and Stone 1990). The concept of privacy itself is not new and it has been generally defined as an individual's ability to control the terms by which their personal information is acquired and used (Westin 1967). A number of behavioral scientists have put emphasis on control when conceptualizing privacy. For example, privacy is viewed as "control over or regulation of or, more narrowly, limitations on or exemption from scrutiny, surveillance, or unwanted access" (Margulis 2003, p. 244). Wolfe and Laufer (1974) noted that control was identified as the psychological concept central to the conceptualization of privacy. Hence, it seems that privacy theorists have applied the term control widely in the privacy literature as the justification for privacy (Johnson 1974). However, privacy theorists have failed to integrate the rich literature on psychological control into their theories of privacy, and consequently the conceptualization of privacy as psychological control has not contributed as much to clarifying the privacy issues as it should have (Margulis 2003). We seek to fill this gap by looking into the privacy concern issue (i.e., loss of control over personal information) from the psychological control perspective in the LBS context.

Since many theories of privacy posit that psychological control is a precondition for protecting privacy (Johnson 1974; Wolfe and Laufer 1974), it follows that the achievement of privacy includes benefits arising from gaining control as such. Numerous studies have demonstrated that a sense of control is a robust predictor of an individual's psychological health and well-being (Bandura 1989). Hence, privacy, as control over private information, supports physical and mental health by providing the opportunities to relax, to be one's self, to emotionally vent, to escape from the stresses, to manage bodily functions, and to cope with loss, shock, and sorrow (Westin 1967). Conversely, privacy failures include costs arising from failures of control over personal information, such as doubts about personal competence, stress, depression, and anxiety (Johnson 1974; Margulis 2003).

In the context of LBS, without the awareness of how their location information is being used and who has access to it, consumers may feel that there is an omnipresent surveillance of their activities by some unknown third party. Consumers' privacy concerns are heightened because of the possibility that some services may not only come as a direct consequence of the ability to identify user location through a mobile device, but also through combining historical records of location data with other personally identifiable information (e.g., name, social security number, purchase history, etc.). Improper handling of such enriched information would result in the discovery and matching of location data and identifiable information to classify the consumers, thereby enhancing the visibility of their behavior and increasing the scope for potentially personally embarrassing situations (Beinat 2001). This may create the conditions for stress and anxiety involved with LBS usage and may further inhibit consumers from using LBS.

Assurance of Control over Personal Information: Fair Information Practices

As an answer to increasing consumer privacy concerns, the U.S. Federal Trade Commission released a set of fair information practices (or FIP as a general term) that highlight several core principles for firms to safeguard consumer's information privacy (FTC 1998). In practice, the FTC has relied on FIP to guide privacy regulation and industry practices via the self-regulation approach in the United States (FTC 1998) and the European Union has subsequently adopted FIP as the heart of its privacy directives (Culnan and Armstrong 1999). Businesses adhering to FIP can lower the privacy concerns associated with the disclosure of personal information through assuring consumers that the firm will abide by a set of rules (Greenberg 1987) and will not behave opportunistically (Shapiro 1987). Although there is some consensus that FIP should be used to empower consumers to control

their personal information, there is no consensus about how they should be implemented to insure the consumer's control (FTC 2000). As stated in Culnan and Bies (2003, p. 331),

> the controversial issue that remains is the appropriate role for legislation, industry self-regulation and technology to insure that the appropriate information regarding a firm's implementation of FIP is available, accurate, and understandable and that consumers have legitimate choices about how their personal information is subsequently used.

In an attempt to unravel this controversial issue, we regard technology, industry self-regulation, and legislation as three different approaches to assure consumer's control over their personal information in the LBS context. Drawing on Yamaguchi's (2001) work on the differentiation of control agents, we hypothesized that consumers are able to exercise personal control or proxy control over their personal information via technology, industry self-regulation, and privacy legislation in the LBS context. The former approach (via technology) refers to the technology-based assurance of control where consumers themselves act as control agents to exercise direct personal control over when and where their personal information is released and subsequently used through their mobile devices. The latter two approaches of control assurance (via self-regulation and legislation) are grouped as institution-based assurance of control where powerful forces (i.e., government legislator and third party intervention) act as the control agents for consumers to exercise proxy control over their personal information.

Hypotheses Development

Technology-Based Assurance of Control

People would especially feel greater autonomy when they exercise direct personal control as the control agent (Yamaguchi 2001). Previous empirical research on employee monitoring has supported the importance of gaining direct personal control in decreasing perceptions of privacy. For instance, Eddy et al. (1999) found that control over the disclosure of information from a human resources information system had a direct effect on privacy concerns. Zweig and Webster (2002, 2003) also found that perceptions of privacy invasion are lower when the monitoring system provides the control feature for employees to control when their images can be displayed. To decrease perceptions of privacy, monitoring system researchers have designed the feature of user control into awareness systems, such as providing users with the option of turning off their awareness cameras (Hudson and Smith 1996).

Similarly, it might be expected that consumers' privacy concerns will be lower when they are empowered with the aid of technologies to exert direct control over personal information in the LBS context. The rapid development of mobile communication and device technologies provides the possibility of building privacy enhancing features into mobile devices. With a mobile device that supports the function of specifying privacy preferences for using LBS applications (Anuket 2003), consumers can exercise personal direct control over personal information with their own hands. Specifically, a mobile consumer is able to control when and where telecommunication operators or merchant service providers can track and communicate with the mobile device in a timely fashion (Anuket 2003). Mobile consumers can turn off the subscribed LBS just by clicking a button on their mobile device anytime they want. Through such a mobile device, the user is able to not only turn the LBS on or off via their mobile phone but also to control the degree of location information released to service providers. Technology-based control also allows the consumer to specify the accuracy to which merchants will be allowed to track the device in time and space (Anuket 2003). For example, the user can specify that service providers can only send wireless advertising messages if the device is within 20 meters of those shops (distance control), and/or with a time delay of 10 minutes within which the past location of the subscriber may be pinpointed (time control). Hence, having such a mobile device with an LBS-related privacy preference specification function should enable consumers to believe that they are able to exercise direct control over the disclosure of personal information.

H1: *Technology-based assurance of control via* ***mobile device*** *in LBS should lead to lower privacy concerns.*

Institution-Based Assurance of Control

When exercise of personal control is neither readily available nor encouraged, one might well relinquish direct control attempts and seek security in proxy control (Bandura 1982). Proxy control is essential for those people who are in a weaker position and thus are unable to change their environment to their liking. Because they do not have enough resources and power to bring about their desired outcome or avoid an undesired outcome in the environment, they cannot afford a means to directly control their

environment other than by aligning with powerful others who can be induced to act for their benefit (Yamaguchi 2001). In our context of LBS, when people perceive that they lack the requisite resources to directly control their personal information disclosed for LBS transactions, they may reshape their decision on using LBS by considering the availability of powerful others who can be induced to act for their benefit. In those situations, the availability of proxy control means that structures such as protective legislation or industry self-regulation are in place to assure that the LBS transaction environment is safe and secure (i.e., the process of conducting an LBS transaction and the subsequent use of consumers' personal information are under control). Hence, with the protective privacy legislation or industry self-regulation in place, government legislators and third party regulators act as proxy agents with the power to regulate the relationship between consumers and service providers with potential or actual conflict of interests.

Institution-Based Assurance of Control via Self-Regulation

One format of institution-based assurance of control over personal information discussed in the literature is industry self-regulation (Culnan and Bies 2003). Self-regulation means that an industry develops rules and enforcement procedures that substitute for government regulation (Swire 1997). For self-regulation to effectively assure consumers' control over the disclosure and subsequent use of their personal information, firms need to voluntarily adopt and implement privacy policies that are based at a minimum on the five elements of FIP (Culnan and Bies 2003). There is also a need for "effective compliance procedures and enforcement mechanisms so that consumers will have the confidence that an organization is playing by the rules, and that there will be negative sanctions for those that do not" (Culnan and Bies 2003, p. 333). Third party intervention, therefore, has been employed in self-regulation to provide legitimacy and trustworthiness to companies through seals of approval that are designed to confirm adequate privacy compliance. Seals of approval from trusted third-parties (such as BBBOnline, Online Privacy Alliance, and TRUSTe) are one example of the mechanism that was created to provide third-party assurances to consumers based on a voluntary contractual relationship between firms and the seal provider. Previous studies have shown that businesses that conform to the industry's self-regulation practices foster consumers' trust and confidence in revealing their personal information and thereby enhance consumers' perceived control over their personal information (Culnan and Armstrong 1999). Hence, having a third party like the reputable TRUSTe to vouch for a firm's trustworthiness should enable consumers to believe that they are able to exercise proxy control over the disclosure and subsequent use of personal information during and after an LBS transaction.

H2: *Institution-based assurance of control via* ***self-regulation*** *in LBS should lead to lower privacy concerns.*

Institution-Based Assurance of Control via Legislation

The second format of institutional-based assurance of control via *legislation* means that relevant legislation is in place to ensure that the disclosure and subsequent use of consumers' personal information is under their own control. Prior sociology and legal literature lend strong support to the positive impact of legislation on the assurance of consumers' control on their personal information (Bandura 1986; Faden et al. 1986). A general civil right of individual integrity, expressed through various doctrines of tort, property, and contract law, protects an individual's freedom of action, ownership, and decision from certain kinds of interference by others (Spiro and Houghteling 1981). The legal system, therefore, is the most powerful mechanism for the exercise of social control since it requires that offenders be punished in order to maintain the deterrent effectiveness of the system (Tittle 1980). Hence, illegal behavior can be deterred through the threat of punishment since the punishment that is actually administered deters illegal behavior (Bandura 1986). Viewing the deterrent effectiveness of a legal system, LBS consumers would believe that the legal assurance of their privacy rights should safeguard them from potential loss of their personal information, which will in turn lead to consumers' confidence in controlling the disclosure and subsequent use of their personal information.

H3: *Institution-based assurance of control via* ***legislation*** *in LBS should lead to lower privacy concerns.*

Privacy Concerns and Intended Use

Along the line of theory of reasoned action (Ajzen and Fishbein 1980), privacy concerns, viewed as a negative antecedent belief, could affect a person's attitude which in turn influences a person's behavioral intention. The negative effect of privacy concerns on behavioral intention has been empirically supported in the e-commerce context (e.g., Chellappa and Sin forthcoming). Hence, we expect a similar negative relationship between privacy concerns and behavioral intention in the LBS context.

H4: *There is a negative relationship between privacy concerns and intention to use LBS.*

Control Variables

Prior research on information privacy and IT acceptance studies suggests a number of additional factors that should be included because of their potential influence on privacy concerns and intention to use LBS.

- *Consumer's general attitude toward LBS* should be viewed as a control variable for the privacy concern construct. Direct marketing literature suggests that the more favorable a consumer's attitude toward direct marketing, the less concerned that consumer will be about information privacy (Phelps et al. 2001).

- *Previous privacy experience* may impact an individual's concerns about information privacy (Stone and Stone 1990) as individuals who have been exposed to or been the victim of personal information abuses should have stronger concerns regarding information privacy (Smith et al. 1996). Hence previous privacy experience is included as the control variable for the privacy concern construct.

- *Innovativeness*, the tendency to learn about or adopt innovations, has been found to have a positive influence on an individual's adoption behavior (Joseph and Shailesh 1984). Innovators are found to be the early adopters of mobile commerce (Pedersen forthcoming).

Figure 1 depicts the research model.

Research Method

The laboratory experiment method is employed because it allows the testing of causal relationships between manipulated and theoretical constructs with minimal interference from extraneous variables. A 2 × 2 × 2 factorial experiment design was employed. In our study, one specific LBS application—the mobile coupon (M-Coupon) service—is utilized as the scenario in our study because it, being one type of push-based LBS, is more controversial in terms of consumers' concerns about privacy and authentication (Levijoki 2001).

Design and Manipulations

The three independent variables—*technology*, *self-regulation*, and *legislation*—were operationalized using the vignette technique, which uses short scenarios in written or pictorial form to elicit perceptions, opinions, beliefs, and attitude to typical situations (Finch 1987). To illustrate how the manipulation of the three independent variables was created, consider the following scenario used in the study:

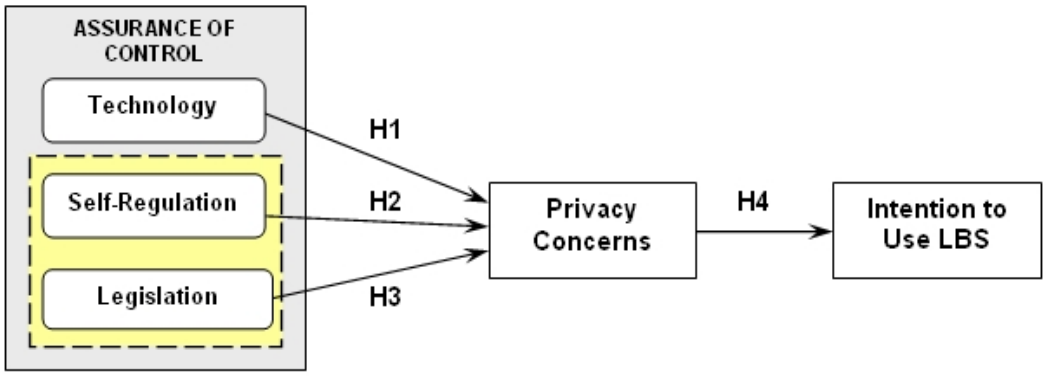


Figure 1. Research Model

> It is 7:00 p.m. on Saturday, and Miss X is with a friend in a restaurant at SuntecCity[1] Mall for dinner. They are discussing what to do after finishing their dinner: shopping, going for drinks in a pub nearby, watching a movie at Cinema B at SuntecCity Mall. At this moment, Miss X's mobile phone is beeping and there is a piece of new message coming to her phone. The message is a coupon delivered from Cinema B: "Top recommendations from Cinema B @ SuntecCity Mall: '*50 First Dates*'! Special discount for today: $4 off for two tickets by using this M-coupon!" Since both Miss X and her friend are very keen to watch this movie, they are going to watch it with the attractive discount after their dinner. Please scroll down to continue as we are going to introduce you the M-Coupon service to which Miss X has subscribed.

According to Havlena and Holbrook (1986, p. 396), the advantage that follows the use of a hypothetical figure (e.g., Miss X, as in the above scenario) in the study design is: "(a) to provide a projective task and thereby discourage social desirability effects, and (b) to avoid problems involving individual differences in reactions to specific types of activities." By adopting the vignette technique, we hope to elicit potential mobile consumers' intention to use LBS when confronted with a need to provide personal information before they can use the services.

We varied the three independent variables—*technology*, *self-regulation*, and *legislation* corresponding to H1, H2 and H3—to construct multiple experiment scenarios. First, *technology* was manipulated by introducing a mobile device with an interactive graphical user interface (see Appendix) for specifying LBS-related privacy preferences. Second, *self-regulation* was manipulated by providing a TRUSTe seal and privacy policy statement on the service provider's website. Finally, *legislation* was manipulated by presenting the subjects with a piece of local news reporting that LBS transactions were governed by a recently activated location privacy protection law. The gist of the location privacy protection act was provided in that piece of news.

Our Web-based experiment system employs the client-side Javascript embedded into the HTML pages. The Javascript codes are programmed to ensure that each subject viewed the treatment conditions before they were allowed to proceed, and to ensure that the subjects answered all the questions before leaving the experiment. These features allow us to be certain that the subjects read the vignette completely before they gave their responses to those questions asking about privacy concerns and intention to use LBS.

Subjects

A total of 256 undergraduate students participated in the experiment (140 females, 116 males). Subjects were volunteers recruited from the business school at a large university in Singapore. As an incentive for their participation, three monetary awards of Singapore $40 per person were raffled among the participants (as of April 2004, one Singapore dollar = 58 U.S. cents). All the subjects own mobile phones and 90 percent reported their ownership as more than one year. Our Web-based experiment system generated the vignette randomly so that each respondent had an equal and independent chance of being put into any of the eight scenarios.

The use of student subjects has sometimes been questioned on grounds of external validity (Gordon et al. 1986). However, we believe that it should not be a major concern in this case because using mobile services has become part and parcel of young people's daily routines (Pedersen forthcoming). Student samples should be closer to the mobile consumer population.

Experiment Procedure

After logging into our Web-based experiment system, all subjects began the experiment by answering questions about their personal information as a form of control check. The subjects were then asked to read the instructions carefully, and to read the descriptions in the vignette carefully. The experimental system logged the accesses made by the subjects to these URLs to ensure that the subjects had actually read the manipulated condition. After having read all the descriptions in the vignette, the subjects were asked to complete a questionnaire regarding privacy concerns and intention to use LBS.

[1]SuntecCity Mall is one of the largest shopping malls in Singapore.

Measures

The subjects were presented with a self-administered questionnaire measuring the two dependent variables: privacy concerns and intention to use LBS. As far as possible, constructs were adapted from existing measurement scales used in prior studies to fit the LBS context where necessary. Table 1 summarizes the questions measuring each construct in this study.

Data Analysis and Results

Manipulation Check

The manipulation on *technology* (TECH), *self-regulation* (SREG), and *legislation* (LEGI) were checked based on seven-point Likert-type scales administered after subjects read the vignette. The results show that all of the treatments were manipulated correctly. First, subjects in the *present technology* treatment group perceived their personal information to be more controllable than did the subjects in the *absent technology* treatment ($t = 15.88$, $p < 0.001$).[2] Second, subjects in the *present self-regulation* treatment group believed that the service provider was less likely to violate their privacy and could protect their data better than did the subjects in *absent self-regulation* treatment ($t = 12.26$, $p < 0.001$).[3] Finally, subjects in *present legislation* treatment group believed that relevant legislation could govern the protection of their private information better than did the subjects in *absent legislation* treatment ($t = 10.02$, $p < 0.001$).[4]

PLS Analyses

Partial least squares (PLS), a second-generation causal modeling statistical technique developed by Wold (1982), was used for data analyses because it possesses many advantages over traditional statistical methods such as factor analysis, ANOVA, and regression. First, it is not contingent upon data having multivariate normal distributions and interval scales (Fornell and Bookstein 1982). This makes PLS suitable for handling manipulated constructs. Second, PLS has the ability to simultaneously test the measurement model and the structural model. This will provide a more complete analysis for the interrelationships in the model. Third, it is generally more appropriate for testing theories in the early stages of development (Fornell and Bookstein 1982). Since this study is an early attempt to advance a theoretical model on consumers' privacy concerns, and intention to adopt LBS, PLS is more suitable for data analysis in this exploratory study.

Testing the Measurement Model

The measurement model was evaluated by examining the convergent and discriminant validity of the research instrument. Convergent validity is the degree to which different attempts to measure the same construct agree (Cook and Campbell 1979). In PLS, three tests are used to determine the convergent validity of measured constructs in a single instrument: reliability of questions, the composite reliability of constructs, and the average variance extracted by constructs. Table 1 presents an assessment of the measurement model. Reliability of these questions was assessed by examining the loading of each question on the construct and the reliability score for all the questions exceeded the criterion of 0.707. Composite reliabilities of constructs with multiple indicators exceeded Nunnally's (1978) criterion of 0.7 while the average variances extracted for these constructs were all above 50 percent and the Cronbach's alphas were also all higher than 0.7. These results of the convergent validity tests provided evi-

[2]The two 7-point Likert scale items used as a manipulation check of *technology* treatment are (1) the mobile device which Miss X uses allows her to control when Telcom B can track and communicate with her device in a timely fashion, and (2) with the mobile device, Miss X has control over specifying the accuracy to which she will allow the service provider to track her device in time and space.

[3]The two 7-point Likert scale items used as a manipulation check of *self-regulation* treatment are (1) the private information that Miss X disclosed for using the M-Coupon service will be kept private and confidential by Company A, and (2) unauthorized third parties will not be able to get access to Miss X's private information.

[4]The two 7-point Likert scale items used as a manipulation check of *legislation* treatment are (1) Miss X knows that relevant legislation will govern the protection of her private information provided for using location-based services and applications, and (2) Miss X knows that the practice of how company A collects, uses, and protects her private information is governed by and interpreted in accordance with the relevant laws.

Table 1. Psychometric Properties of the Measurement Model

Measures of Constructs and Sources (measured on seven-point, Likert-type scale)	**Loading**	**CA**	**CR**	**AVE**
Privacy Concerns (PC) (Dinev and Hart 2004; Smith et al. 1996) If you were Miss X, please indicate the extent to which you agree with the following statements:		0.902	0.923	0.633
• I am concerned that the service providers may keep private location information in a non-secure manner (**PC-1**)	0.782			
• I am concerned that the service providers may not take measures to prevent unauthorized access to my location information (**PC-2**)	0.798			
• I am concerned that the service providers may divulge my location information to unauthorized parties without my consent (**PC-3**)	0.838			
• I am concerned that the service providers may use my location information for other purposes, e.g., analyzing my daily activities to derive information about me (**PC-4**)	0.744			
• I am concerned that the service providers may share my location information with other companies without notifying me or getting my authorization (**PC-5**)	0.845			
• I am concerned that the service providers may sell my location information to other companies without notifying me or getting my authorization (**PC-6**)	0.840			
• I am concerned about providing personal location information to use LBS, because it could be in a way I did not foresee (**PC-7**)	0.710			
Intention to Use LBS (INT)(Gefen et al. 2003) The following questions are about *your general intention to use LBS*. Please rate the extent to which *you* agree with the following statement:		0.954	0.974	0.858
• I am very likely to provide the LBS service provider with my personal information it needs to better serve my needs in the next 12 months (**INT-1**)	0.890			
• I would disclose my personal information to use this type of LBS from the service provider in the next 12 months (**INT-2**)	0.906			
• I intend to use this type of LBS in the next 12 months (**INT-3**)	0.942			
• I predict I would use this type of LBS in the next 12 months (**INT-4**)	0.926			
• I plan to use this type of LBS in the next 12 months (**INT-5**)	0.931			
General Attitude toward LBS (ATT) (Okechuku and Wang 1988) Please scale your attitude towards general LBS based on your current knowledge:		0.852	0.909	0.770
• In general, LBS are attractive (**ATT-1**)	0.883			
• In general, LBS are useful (**ATT-2**)	0.855			
• In general, LBS are valuable (**ATT-3**)	0.894			
Innovativeness (**INNV**) (Joseph and Shailesh 1984)		0.828	0.901	0.751
• I like to try new and different things (**INNV-1**)	0.853			
• I often try new things before my friends and neighbors do (**INNV-2**)	0.866			
• I like to experiment with new ways of doing things (**INNV-3**)	0.881			
Previous Privacy Experience (**PPRV**) (Smith et al. 1996)		0.762	0.865	0.683
• How often have you personally experienced incidents whereby your personal information was used by some service provider or e-commerce website without your authorization? (1 = Not at all; 7= Very often) (**PPRV-1**)	0.887			
• How often have you personally been the victim of what you felt was an improper invasion of privacy? (1 = Not at all; 7 = Very often) (**PPRV-2**)	0.872			
• How much have you heard or read during the last year about the use and potential misuse of consumer's personal information without consumer's authorization by some service provider or e-commerce website? (1 = Not at all; 7 =Very much) (**PPRV-3**)	0.709			

(**CA:** Cronbach's Alpha; **CR:** Composite Reliability; **AVE:** Average Variance Extracted)

Table 2. Discriminant Validity of Constructs

Construct	PC	INT	ATT	INNV	PPRV
PC	0.795				
INT	-0.263	0.926			
ATT	-0.085	0.596	0.877		
INNV	-0.034	0.431	0.343	0.867	
PPRV	0.300	-0.105	-0.053	0.020	0.827

dence for convergent validity of the measurement model. Discriminant validity is the degree to which measures of different constructs are distinct (Campbell and Fiske 1959). To test discriminant validity, the square root of the variance shared between a construct and its measures should be greater than the correlations between the construct and any other construct in the model. Table 2 reports the results of discriminant validity, which is checked by comparing the diagonal to the non-diagonal elements. All items fulfilled the requirement of discriminant validity.

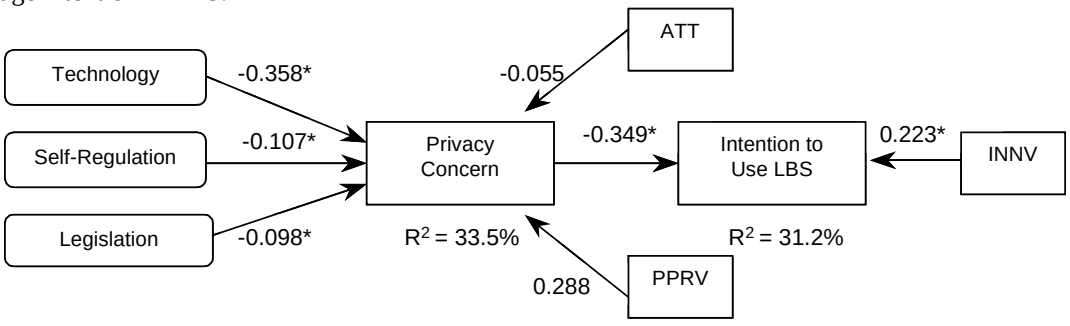
Testing the Structural Model

With adequacy in the measurement model affirmed, the PLS structural model was next examined to assess its explanatory power and the significance of the hypothesized paths. The explanatory power of the structural model was assessed based on the amount of variance in the endogenous construct (intention to use LBS) for which the model could account. Our structural model can explain 31.2 percent of the variance for intention to use LBS. Since all hypotheses are unidirectional, they were tested with one-tailed t-tests at 5 percent significance level. Figure 2 depicts the structural model.

Each hypothesis (H1 to H4) corresponded to a path in the structural model. Bootstrapping technique was applied to obtain the corresponding t-values in order to assess the significance of the path estimates. Privacy concern (H4) was a significant predictor of intention to use LBS, and technology (H1), self-regulation (H2), and legislation (H3) were the significant predictors of privacy concern. Therefore, all the hypotheses were supported.

Discussion and Conclusions

This research constitutes one of the first systematic empirical studies to identify the antecedents to privacy concerns by incorporating psychological control with privacy literature in an LBS context, an important area that has not been comprehensively examined by previous privacy theorists (Margulis 2003). Consistent with previous findings (Beinat 2001; Gidari 2000), the evidence from this study provided empirical support that privacy concern is a major inhibiting factor in consumers' adoption of LBS. Our proposed model is able to account for 31.2 percent of the variances in usage intention, which possesses enough explanatory power to make the interpretation of path coefficients meaningful. Thus, privacy concern is shown to have a negative impact on usage intention in LBS.



*Significant at 5% level of significance.

Figure 2. Results of PLS Analyses for Theoretical Model

Furthermore, our findings help provide some initial insights into the controversial issues surrounding the role of technology, industry self-regulation, and legislation in bearing the responsibility of assuring consumer privacy. In particular, our three proposed assurance controls to assuage privacy concerns—technology, industry self-regulation, and legislation—are able to account for 33.5 percent of the variances in privacy concerns. This shows that consumers did regard the availability of technology, self-regulation, or legislation on assuring control over personal information as important measures that could alleviate privacy concerns in LBS. Hence, it appears that the marriage of the privacy and psychological control literature streams should provide a rich understanding of the antecedents to privacy concerns of LBS consumers.

The negative impacts of the three different approaches of control assurance on privacy concerns were shown to be significant. By making a comparison among the roles of technology versus industry regulator versus government legislator, it is apparent that mobile consumers expect technology to play a more active role in assuring their control over personal information. This finding confirms that consumers perceive a lower level of privacy concerns when they themselves act as the control agent to exercise direct personal control compared to when the third party or government legislator acts as the proxy agent to exercise proxy control.

Examining control variables in the structural model also offers some insight into the factors affecting consumers' intention to use LBS. Consumer's general attitude toward LBS and previous privacy experience were shown to have no effects on privacy concerns in our study while subject innovativeness has been found significant in influencing LBS usage intention. It seems that innovators are likely to pay more attention to LBS than the majority and laggards do.

This study suggests a number of opportunities for further research. Some of these relate directly to overcoming the limitations of this study. First, the relationships between privacy concerns and intention are likely more complex than suggested by the current research model. There are other aspects such as fairness, technology acceptance, and trust that may affect privacy concerns and adoption intention as suggested by prior literature (Gefen et al. 2003; Zweig and Webster 2002), which could also be examined in future research. Second, other than treating innovativeness as the control variable for intention, it is likely that innovativeness may moderate the relationship between privacy concerns and adoption intention. Opportunities exist to explore this moderating relationship and other personality variables (Zweig and Webster 2003) as moderators of intention. Third, the scenarios used in the study represent an over-simplification of LBS and were relatively favorable, which may limit the generalizability of our findings. Future work could be directed to look into the applicability of our findings to different LBS applications and to see if manipulating the description along the dimensions of usefulness–annoyance would influence the results. The challenge is to continue improving the experiment design which could be a scenario where consumers really are on the move. Field research along the direction of this study could certainly contribute significantly to fostering the acceptance of LBS.

Our findings have important practical implications for the various players in the LBS landscape: merchants, privacy advocates, government legislators, wireless service providers, and mobile device manufacturers. The results seem to suggest that privacy advocates and government regulators should not tar privacy issues in LBS with a broad brush. While basic protections via institution-based approaches of control assurance (i.e., industry self-regulation and legislation) would be necessarily beneficial for consumers, they are not suited for ensuring that each individual is able to choose the level of privacy that he or she desires. With the rapid advancement of positioning technology and social conditions, such a "one-size-fits-all," static approach to assure privacy is unable to quickly or accurately accommodate the interests of each individual or broad group of users (Anuket 2003). By contrast, a dynamic approach that assures control over personal information in the hands of LBS consumers seems more attractive. Hence, it is very important for wireless service providers and mobile device manufacturers to develop improved devices with user-friendly interfaces for specifying privacy preferences to counter privacy concerns. We may conclude that with minimum protections via industry privacy self-regulation and relevant privacy legislation in place, the technology-based assurance of control over personal information would be more flexible to respond to consumer desires and marketplace conditions.

Overall, this exploratory study examines the critical privacy issues in an LBS context using an experimental approach. Through the causal modeling of the antecedents affecting usage intentions in LBS, our findings provide preliminary empirical support to understand the privacy issues from a psychological control perspective. This study has also shed some light on the controversial issues surrounding the role of technology, industry self-regulation, and legislation in bearing the responsibility of assuring consumer privacy. We believe that, using the groundwork laid down in this study, future research along these directions could contribute significantly to making LBS an important and profitable mobile commerce application.

References

Ajzen, I., and Fishbein, M. *Understanding Attitudes and Predicting Social Behavior*, Prentice-Hall, Englewood Cliffs, NJ, 1980.

Anuket, B. *User Controlled Privacy Protection in Location-Based Services*, Unpublished Master's Thesis, Department of Spatial Information Science and Engineering, University of Maine, Orono, ME, 2003.

Bandura, A. "Human Agency in Social Cognitive Theory," *American Psychologist* (44), 1989, pp. 1175-1184.

Bandura, A. "Self-Efficacy Mechanism in Human Agency," *American Psychologist* (37), 1982, pp. 122-147.

Bandura, A. *Social Foundations of Thought and Action: A Social Cognitive Theory*, Prentice-Hall, Englewood Cliffs, NJ, 1986.

Beinat, E. "Privacy and Location-Based: Stating the Policies Clearly," *GeoInformatics*, September 2001 (available online at . **http://www.geodan.nl/nl/geodan/nieuws/pdf/GeoInformatics_sept_2001_LBSandPrivacy.pdf**; accessed September 6, 2004).

Campbell, D. T., and Fiske, D. W. "Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix," *Psychological Bulletin* (56:1), 1959, pp. 81-105.

Chellappa, R. K., and Sin, R. "Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management*, forthcoming (available online at **http://asura.usc.edu/~ram/rcf-papers/per-priv-itm.pdf**; accessed September 6, 2004).

Cook, M., and Campbell, D. T. *Quasi-Experimentation: Design and Analysis Issues for Field Settings*, Houghton Mifflin, Boston, 1979.

Culnan, M. J., and Armstrong, P. K. "Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), January-February 1999, pp. 104-115.

Culnan, M. J., and Bies, J. R. "Consumer Privacy: Balancing Economic and Justice Considerations," *Journal of Social Issues* (59:2), 2003, pp. 323-342.

Dinev, T., and Hart, P. "Privacy Concerns and Internet Use—A Model of Trade-off Factors," Working Paper, Department of Information Technology and Operations Management, Florida Atlantic University, 2004.

Eddy, R. E., Stone, L. D., and Stone-Romero, F. E. "The Effects of Information Management Polices on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives," *Personnel Psychology* (52), 1999, pp. 335-358.

Faden, R. R., Beauchamp, L. T., and King, P. M. N. *A History and Theory of Informed Consent*, Oxford University Press, New York, 1986.

Finch, J. "The Vignette Technique in Survey Research," *Sociology* (21), 1987, pp. 105-114.

FTC. *Privacy Online: Fair Information Practices in the Electronic Marketplace*, Federal Trade Commission, Washington, DC, May 2000 (available online at **http://www.ftc.gov/reports/privacy2000/privacy2000.pdf**; accessed September 6, 2004).

FTC. *Privacy Online: A Report to Congress*, Federal Trade Commission, Washington, DC, June 1998 (available online at **http://www.ftc.gov/reports/privacy3/priv-23a.pdf**; accessed September 6, 2004).

Fornell, C., and Bookstein, F. L. "Two Structual Equation Models: LISREL and PLS Applied to Customer Exit-Voice Theory," *Journal of Maketing Research* (19:11), 1982, pp. 440-452.

Gefen, D., Karahanna, E., and Straub, D. W. "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly* (27:1), March 2003, pp. 51-90.

Gidari, A. "No 'L-Commerce[SM]' Without 'L-Privacy': Fair Location Information Practices for Mobile Commerce," paper presented at L-Commerce 2000—The Location Services & GPS Technology Summit, Washington, DC, May 2000.

Gordon, M. E., Slade, A. L., and Schmitt, N. "The 'Science of the Sophomore' Revisited: From Conjecture to Empiricism," *Academy Management Review* (11:1), 1986, pp. 191-207.

Greenberg, J. "A Taxonomy of Organizational Justice Theories," *Academy of Management Review* (12:1), 1987, pp. 9-22.

Greenberger, B. D., and Strasser, S. "Development and Application of a Model of Personal Control in Organizations," *Academy of Management Review* (11:1), 1986, pp. 164-177.

Havlena, W. J., and Holbrook, B. M. "The Varieties of Consumption Experience: Comparing Two Typologies of Emotion in Consumer Behavior," *Journal of Consumer Research* (13), 1986, pp. 394-404.

Hudson, S. E., and Smith, I. "Techniques for Addressing Fundamental Privacy and Disruption Tradeoffs in Awareness Support Systems," in *Proceedings of Computer Supported Cooperative Work '96 Conference*, ACM Press, New York, 1996, pp. 248-257.

Joseph, B., and Shailesh, J. V. "Concurrent Validity of a Measure of Innovative Cognitive Style," *Journal of the Academy of Marketing Science* (12), Spring 1984, pp. 159-175.

Johnson, C. A. "Privacy as Personal Control," in *Man-Environment Interactions: Evaluations and Applications: Part 2, Volume 6, Privacy*, S. T. Margulis (Ed.), Environmental Design Research Association, Washington, DC, 1974, pp. 83-100.

Langer, E. J. "The Illusion of Control," *Journal of Personality and Social Psychology* (32), 1975, pp. 311-328.

Latane, B., and Darley, J. M. *The Unresponsive Bystander: Why Doesn't He Help?*, Appleton-Century-Crofts, New York, 1970.

Levijoki, S. "Privacy vs Location Awareness," Working Paper, Department of Computer Science, Helsinki University of Technology, January 2001 (available online at **http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/papers/levijoki.pdf**; accessed September 6, 2004).

Margulis, T. S. "Privacy as a Social Issue and Behavioral Concept," *Journal of Social Issues* (59:2), 2003, pp. 243-261.
Nunnally, J. C. *Psychometric Theory* (2nd ed.), McGraw-Hill, New York, 1978.
Okechuku, C., and Wang, G. "The Effectiveness of Chinese Print Advertisement in North America," *Journal of Advertising Research* (28), October/November 1988, pp. 25-34.
Pedersen, E. P. "Adoption of mobile Internet Services: An Exploratory Study of Mobile Commerce Early Adopters," *Journal of Organizational Computing and Electronic Commerce*, forthcoming (available online at **http://ikt.hia.no/perep/earlyadopt_paper2.pdf**; accessed September 6, 2004).
Phelps, E. J., Souza, G., and Nowak, J. G. "Antecedents and Consequences of Consumer Privacy Concerns: An Empirical Investigation," *Journal of Interactive Marketing* (15:4), 2001, pp. 2-17.
Shapiro, S. P. "The Social Control of Impersonal Trust," *American Journal of Sociology* (93:3), 1987, pp. 623-658.
Sharma, S., and Deng X. "An Empirical Investigation of Factors Affecting the Acceptance of Personal Digital Assistance by Individuals," in *Proceeding of 8th Americas Conference on Information Systems*, R. Ramsower and J. Windsor (Eds.), Dallas, TX, August 2002, pp. 1829-1834.
Skinner, E. A. "A Guide to Constructs of Control," *Journal of Personality and Social Psychology* (71), 1996, pp. 549-570.
Skinner, E. A., Chapman, M., and Baltes, P. B. "Control, Means-Ends, and Agency Believes: A New Conceptualization and its Measurement During Childhood," *Journal of Personality and Social Psychology* (54), 1988, pp. 117-133.
Smith, H. J., Milberg, J. S., and Burke, J. S. "Information Privacy: Measuring Individuals' Concerns about Organizational Practices," *MIS Quarterly* (20: 2), June 1996, pp. 167-196.
Spiro, W. G., and Houghteling, L. J. *The Dynamics of Law* (2nd ed.), Harcourt Brace Jovanovich, New York, 1981.
Stone, E. F., and Stone D. L. "Privacy in Organizations: Theoretical Issues, Research Findings, and Protection Mechanisms," *Research in Personnel and Human Resources Management* (8:3), 1990, pp. 349-411.
Swire, P. P. "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information," *Privacy and Self-Regulation in the Information Age*, U.S. Department of Commerce, Department of Commerce, Washington, DC, 1997, pp. 3-19.
Tittle, C. R. *Sanctions and Social Deviance: The Question of Deterrence*, Praeger, New York, 1980.
Westin, A. F. *Privacy and Freedom*, Atheneum, New York, 1967.
Wold, H. "Soft Modeling: The Basic Design and Some Extensions," in *Systems Under Indirect Observations: Part 2*, K.G. Joreskog and H. Wold (Eds.), North-Holland, Amsterdam, 1982, pp. 1-54
Wolfe, M., and Laufer, R. S. "The Concept of Privacy in Childhood and Adolescence," in *Privacy as a Behavioral Phenomenon*, S. T. Margulis (Ed.), Symposium Presented at the Meeting of the Environmental Design Research Association, Milwaukee, WI, May 1974.
Yamaguchi, S. "Culture and Control Orientations," in *The Handbook of Culture and Psychology*, D. Matsumoto (Ed.), Oxford University Press, New York, 2001, pp. 223-243.
Zweig, D., and Webster, J. "Personality as a Moderator of Monitoring Acceptance," *Computers in Human Behavior* (19), 2003, pp. 479-493.
Zweig, D., and Webster, J. "Where is the Line between Benign and Invasive? An Examination of Psychological Barriers to the Acceptance of Awareness Monitoring Systems," *Journal of Organizational Behavior* (23), 2002, pp. 605-633.

Appendix

Screenshots of the Mock Mobile Device with an Interactive Graphical User Interface for Specifying Privacy Preferences Manipulated in the Experiment (adapted from Anuket 2003).

Figure I.
On/Off LBS Preference

Figure II.
Distance Preference

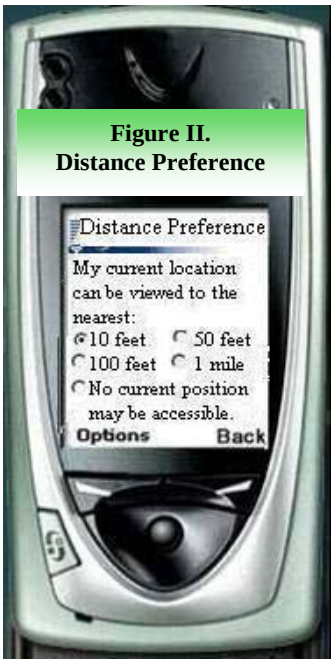


Figure III.
Time Delay Preference